Technical Cybersecurity

Attack Surface Analysis

Attack surfaces can be analyzed offensively and defensively.

Analysis

Attackers have specific goals

- Device control, credentials, data, etc.

So do defenders

- Defenders want to eliminate vectors
- Eliminate, block, reduce risk, secure, etc.

The are not the same, but one informs the other.

Attacker Analysis

Goals

- Depends upon the campaign, usually predefined
- Can change, sub-goals are relatively ad-hoc

Vulnerabilities

- We have a vector, but is it vulnerable?
- …usually no.

Exploits

- We've found a vector with a vulnerability; is it exploitable?
- …usually no here too

Defender Analysis

Value

- Things that are important; system or data
- Don’t know exactly what attackers will want
- …but usually know what in the system has value

Vulnerabilities

- You know attack vectors; are they vulnerable or exploitable?
- …they might be in the future.

Controls

- Manage your attack surface, apply controls to vectors, close off, etc.

Let’s revisit our smart bulb.